In the Claims:

Please cancel claims 1-44, and please add claims 45-88, as shown below.

1. – 44. (Canceled)

45. (New) A computer-implemented method, comprising:

storing access control information for a particular node of a tree of nodes representing entities managed by a directory server, wherein the access control information comprises at least one macro entry;

in response to a request from a requester for a directory server operation targeted at a node of the tree,

generating an expanded version of the access control information using the at least one macro entry, wherein the expanded version comprises additional information derived from one or more attributes stored at the directory server;

determining whether the requester has permission for the directory server operation, wherein said determining comprises comparing at least a portion of the expanded version of the access control information with one or more attribute values of the requester;

in response to determining that the requester has permission, performing the directory server operation; and

in response to determining that the requester does not have permission, providing a failure indication to the requester.

46. (New) The method as recited in claim 45, wherein the expanded version is derived at least in part by replacing the at least one macro entry with at least one substitute string derived from the one or more attributes stored at the directory server.

47. (New) The method as recited in claim 45, wherein the request is targeted at the particular node, and wherein the additional information is derived from one or more attributes of the particular node.

48. (New) The method as recited in claim 45, wherein the particular node is a root node of a subtree of other nodes of the tree, wherein the request is targeted at an other node of the subtree, and wherein the additional information is derived from one or more attributes of the other node.

49. (New) The method as recited in claim 45, wherein said determining whether the requester has permission for the directory server operation comprises determining whether an attribute value of the requester matches an attribute value specified in the expanded version of the access control information.

50. (New) The method as recited in claim 48, wherein said generating the expanded version comprises adding a plurality of fields to the access control information, wherein said determining whether the requester has permission for the directory server operation comprises:

in response to determining that the attribute value of the requester does not match the expanded version, modifying the expanded version by removing at least one field of the plurality of fields from the expanded version; and

determining whether an attribute value of the requester matches an attribute value specified in the modified expanded version of the access control information.

51. (New) The method as recited in claim 45, wherein the access control information comprises two or more macro entries, including a target macro entry in a portion of the access control information identifying a target object to which access is to be controlled, and a subject macro entry in a portion of the access control information specifying attributes of requesters to whom access is to be provided.

52. (New) The method as recited in claim 51, wherein said generating the expanded version comprises replacing the target macro entry with a first substitute string, and replacing the subject macro entry with a second substitute string derived from the first substitute string.

53. (New) The method as recited in claim 45, wherein the at least one macro entity identifies an attribute name, wherein the additional information comprises at least one string derived from a value of an attribute identified by the attribute name.

54. (New) The method as recited in claim 53, wherein the attribute identified by the attribute name is a multi-valued attribute, wherein the directory server stores at least a first value and a second value for the multi-valued attribute for the node targeted by the request, wherein the additional information comprises the first value of the multi-valued attribute, wherein said determining whether the requester has permission comprises:

comparing a portion of the expanded version including the first value with the requester's value of the multi-valued attribute;

in response to determining that the portion of the expanded version does not match the requester's value, generating a second expanded version of the access control information by replacing the first value of the multi-valued attribute in the expanded version with the second value of the multi-valued attribute; and

comparing a portion of the second expanded version including the second value with the requester's value of the multi-valued attribute.

55. (New) The method as recited in claim 45, wherein the additional information is derived from a distinguished name of a node of the tree.

56. (New) The method as recited in claim 45, wherein the at least one macro entry is included within a portion of the access control information that identifies a distinguished name of a group of entities defined at the directory server.

57. (New) The method as recited in claim 45, wherein the at least one macro entity is included within a portion of the access control information that identifies a distinguished name of a role defined at the directory server.

58. (New) The method as recited in claim 45, wherein the at least one macro entity is included within a portion of the access control information that identifies at least one of: a distinguished name of a user identified at the directory server, and a user attribute defined at the directory server.

59. (New) The method as recited in claim 45, wherein the at least one macro entity is included within a portion of the access control information that specifies a target filter used by the directory server to select nodes to which the access control information applies.

60. (New) A system, comprising:

a processor;

a memory coupled to the processor, wherein the memory stores program instructions executable by the processor to:

store access control information for a particular node of a tree of nodes representing entities managed by a directory server, wherein the access control information comprises at least one macro entry;

in response to a request from a requester for a directory server operation targeted at a node of the tree,

generate an expanded version of the access control information using the macro entry, wherein the expanded version includes additional information derived from one or more attributes stored at the directory server;

determining whether the requester has permission for the directory server operation, wherein said determining comprises comparing at least a portion of the expanded version of the access control information with one or more attribute values of the requester;

in response to determining that the requester has permission, perform the directory server operation; and

in response to determining that the requester does not have permission, provide a failure indication to the requester.

61. (New) The system as recited in claim 60, wherein the expanded version is derived at least in part by replacing the at least one macro entry with at least one substitute string derived from the one or more attributes stored at the directory server.

62. (New) The system as recited in claim 61, wherein the request is targeted at the particular node, and wherein the additional information is derived from one or more attributes of the particular node.

63. (New) The system as recited in claim 60, wherein the particular node is a root node of a subtree of other nodes of the tree, wherein the request is targeted at an other node of the subtree, and wherein the additional information is derived from one or more attributes of the other node.

64. (New) The system as recited in claim 60, wherein said determining whether the requester has permission for the directory server operation comprises determining whether an attribute value of the requester matches an attribute value specified in the expanded version of the access control information.

65. (New) The system as recited in claim 64, wherein the additional information comprises a plurality of fields, wherein said determining whether the requester has permission for the directory server operation comprises:

in response to determining that the attribute value of the requester does not match the expanded version, modifying the expanded version by removing at least one field of the plurality of fields from the expanded version; and

determining whether an attribute value of the requester matches an attribute value specified in the modified expanded version of the access control information.

66. (New) The system as recited in claim 60, wherein the access control information comprises two or more macro entries, including a target macro entry in a portion of the access control information identifying a target object to which access is to be controlled, and a subject macro entry in a portion of the access control information specifying attributes of requesters to whom access is to be provided.

67. (New) The system as recited in claim 66, wherein said generating the expanded version comprises replacing the target macro entry with a first substitute string,

and replacing the subject macro entry with a second substitute string derived from the first substitute string.

68. (New) The system as recited in claim 60, wherein the at least one macro entity identifies an attribute name, wherein the additional information is derived from a value of an attribute identified by the attribute name.

69. (New) The system as recited in claim 68, wherein the attribute identified by the attribute name is a multi-valued attribute, wherein the directory server stores at least a first value and a second value for the multi-valued attribute for the node targeted by the request, wherein the additional information comprises the first value of the multi-valued attribute, wherein said determining whether the requester has permission comprises:

comparing a portion of the expanded version including the first value with the requester's value of the multi-valued attribute;

in response to determining that the portion of the expanded version does not match the requester's value, generating a second expanded version of the access control information by replacing the first value of the multi-valued attribute in the expanded version with the second value of the multi-valued attribute; and

comparing a portion of the second expanded version including the second value with the requester's value of the multi-valued attribute.

70. (New) The system as recited in claim 60, wherein the additional information is derived from a distinguished name of a node of the tree.

71. (New) The system as recited in claim 60, wherein the at least one macro entry is included within a portion of the access control information that identifies a distinguished name of a group of entities defined at the directory server.

72. (New) The system as recited in claim 60, wherein the at least one macro entity is included within a portion of the access control information that identifies a distinguished name of a role defined at the directory server.

73. (New) The system as recited in claim 60, wherein the at least one macro entity is included within a portion of the access control information that identifies at least one of: a distinguished name of a user identified at the directory server, and a user attribute defined at the directory server.

74. (New) The system as recited in claim 60, wherein the at least one macro entity is included within a portion of the access control information that specifies a target filter used by the directory server to select nodes to which the access control information applies.

75. (New) A tangible, computer-readable medium, comprising program instructions, wherein the instructions are computer-executable to:

store access control information for a particular node of a tree of nodes representing entities managed by a directory server, wherein the access control information comprises at least one macro entry;

in response to a request from a requester for a directory server operation targeted at a node of the tree,

generate an expanded version of the access control information using the at least one macro entry, wherein the expanded version includes additional information derived from one or more attributes stored at the directory server;

determining whether the requester has permission for the directory server operation, wherein said determining comprises comparing at least a portion of the expanded version of the access control information with one or more attribute values of the requester;

in response to determining that the requester has permission, perform the directory server operation; and

in response to determining that the requester does not have permission, provide a failure indication to the requester.

76. (New) The computer-readable medium as recited in claim 75, wherein the expanded version is derived at least in part by replacing the at least one macro entry with at least one substitute string derived from the one or more attributes stored at the directory server.

77. (New) The computer-readable medium as recited in claim 75, wherein the request is targeted at the particular node, and wherein the additional information is derived from one or more attributes of the particular node.

78. (New) The computer-readable medium as recited in claim 75, wherein the particular node is a root node of a subtree of other nodes of the tree, wherein the request is targeted at an other node of the subtree, and wherein the additional information is derived from one or more attributes of the other node.

79. (New) The computer-readable medium as recited in claim 75, wherein said determining whether the requester has permission for the directory server operation comprises determining whether an attribute value of the requester matches an attribute value specified in the expanded version of the access control information.

80. (New) The computer-readable medium as recited in claim 79, wherein the at additional information comprises a plurality of fields, wherein said determining whether the requester has permission for the directory server operation comprises:

in response to determining that the attribute value of the requester does not match the expanded version, modifying the expanded version by removing at least one field of the plurality of fields from the expanded version; and

determining whether an attribute value of the requester matches an attribute value specified in the modified expanded version of the access control information.

81. (New) The computer-readable medium as recited in claim 75, wherein the access control information comprises two or more macro entries, including a target macro entry in a portion of the access control information identifying a target object to which access is to be controlled, and a subject macro entry in a portion of the access control information specifying attributes of requesters to whom access is to be provided.

82. (New) The computer-readable medium as recited in claim 81, wherein said generating the expanded version comprises replacing the target macro entry with a first substitute string, and replacing the subject macro entry with a second substitute string derived from the first substitute string.

83. (New) The computer-readable medium as recited in claim 75, wherein the at least one macro entity identifies an attribute name, wherein the additional information is derived from a value of an attribute identified by the attribute name.

84. (New) The computer-readable medium as recited in claim 83, wherein the attribute identified by the attribute name is a multi-valued attribute, wherein the directory server stores at least a first value and a second value for the multi-valued attribute for the node targeted by the request, wherein the additional information comprises the first value

of the multi-valued attribute, wherein said determining whether the requester has permission comprises:

comparing a portion of the expanded version including the first value with the requester's value of the multi-valued attribute;

in response to determining that the portion of the expanded version does not match the requester's value, generating a second expanded version of the access control information by replacing the first value of the multi-valued attribute in the expanded version with the second value of the multi-valued attribute; and

comparing a portion of the second expanded version including the second value with the requester's value of the multi-valued attribute.

85. (New) The computer-readable medium as recited in claim 75, wherein the additional information is derived from a distinguished name of a node of the tree.

86. (New) The computer-readable medium as recited in claim 75, wherein the at least one macro entry is included within a portion of the access control information that identifies a distinguished name of a group of entities defined at the directory server.

87. (New) The computer-readable medium as recited in claim 75, wherein the at least one macro entity is included within a portion of the access control information that identifies a distinguished name of a role defined at the directory server.

88. (New) The computer-readable medium as recited in claim 75, wherein the at least one macro entity is included within a portion of the access control information that identifies at least one of: a distinguished name of a user identified at the directory server, a user attribute defined at the directory server, and a target filter used by the directory server to select nodes to which access control information applies.